Cybersecurity Hygiene for Everyone

2025 Clergy-Laity Assembly
Metropolis of Atlanta

Outline

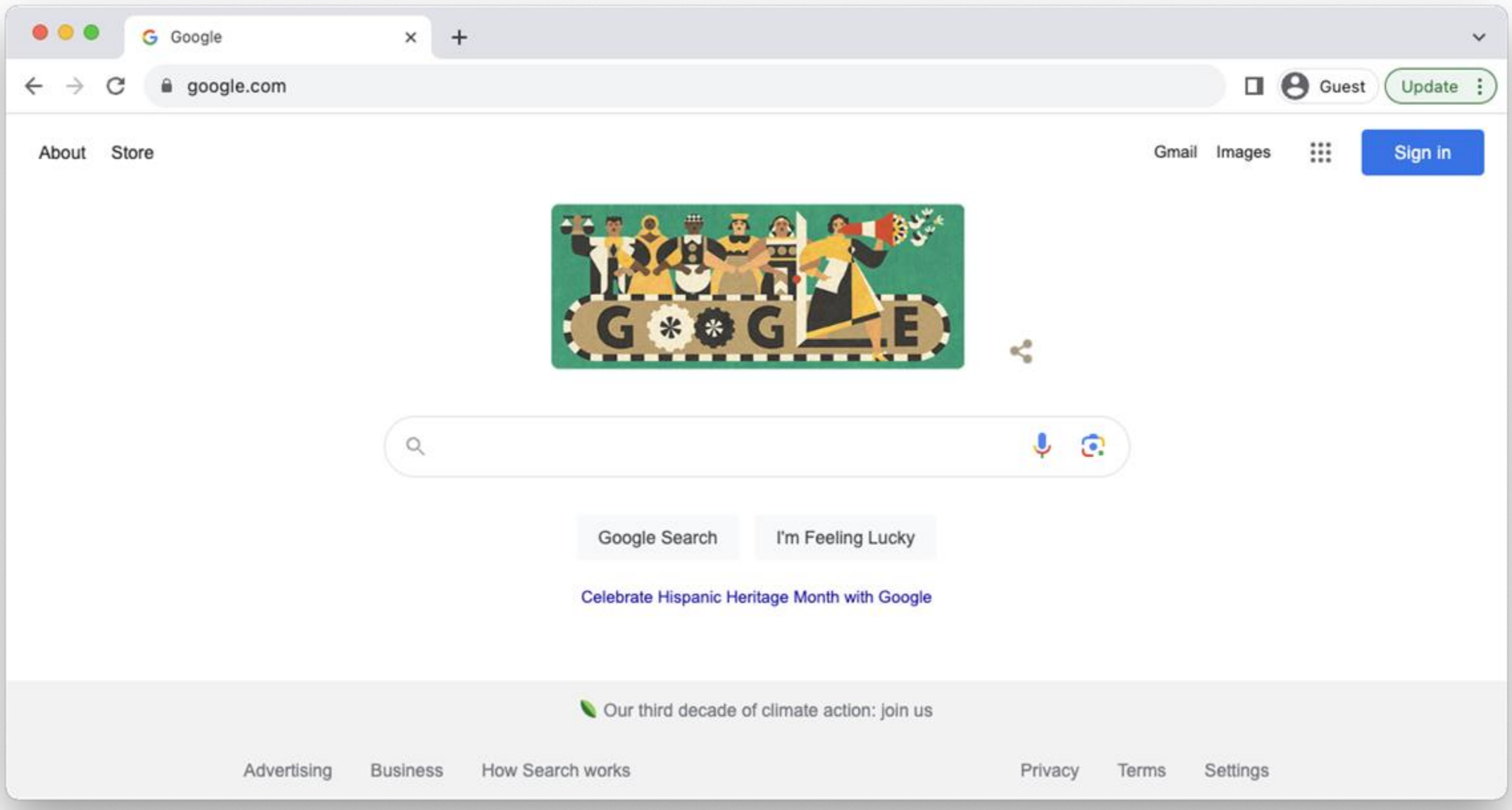
- Introduction
- Low hanging fruit for cyber protection
- Brief introduction to the browser, and URL structure
- Cybersecurity Best Practices & Use Cases

Introduction

- Andy Green, Ph.D.
- Parish Council Member, Holy Transfiguration, Marietta
- Chair – Cybersecurity Committee, Metropolis of Atlanta
- Chair – Parish Cybersecurity Subcommittee, Archdiocese of America
- Assistant Professor, Kennesaw State University
- Anything I say is my own opinion and does not represent KSU or the University System of Georgia

Low Hanging Fruit

- Don’t buy gift cards
- Don’t buy/ send Cryptocurrency
- Use Multi Factor Authentication (MFA)
- Don’t share MFA codes
- Don’t let unknown people control your computer


Google
google.com
Guest
Update
About
Store
Gmail
Images
Sign in
Google Search
I'm Feeling Lucky
Celebrate Hispanic Heritage Month with Google
Our third decade of climate action: join us
Advertising
Business
How Search works
Privacy
Terms
Settings

How a URL works:

www.photos.google.com

Subdomain

Top Level Domain

Domain

How scammers use this

Malicious URL:

www.google.ml.com

Valid URL:

www.support.google.com

How scammers use this

Malicious URL:

www.wellsfarg0.com

Valid URL:

www.wellsfargo.com

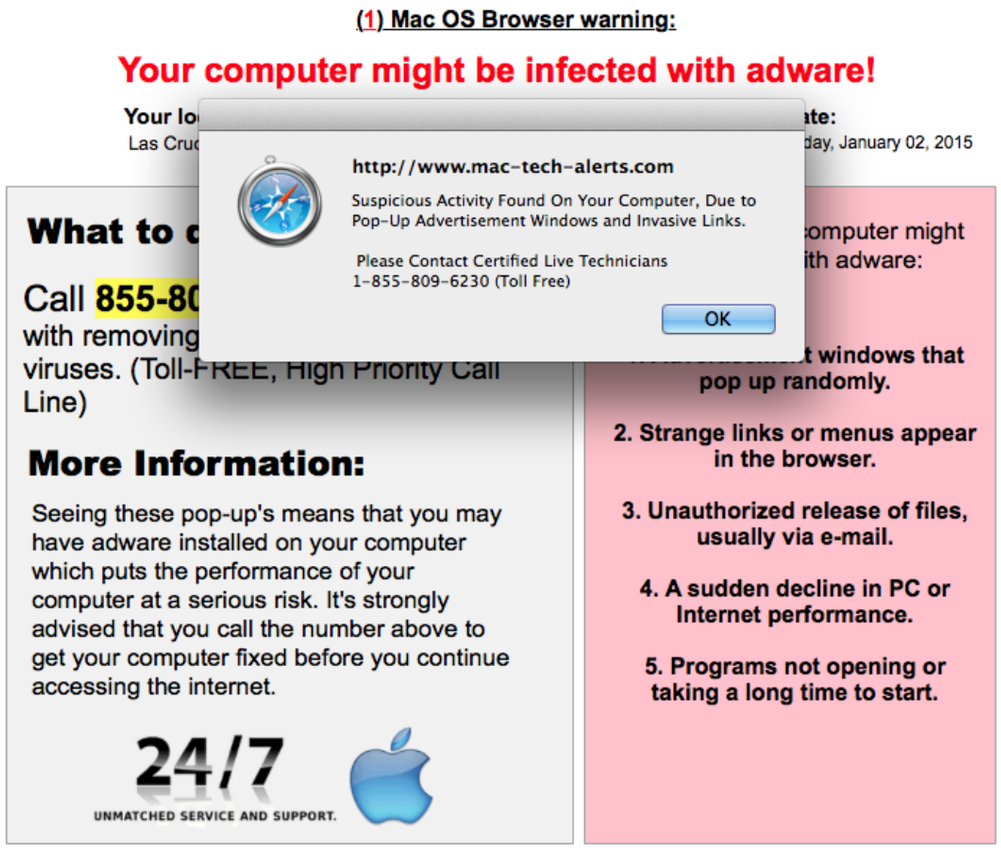
Entering private or sensitive information?

Look for the lock

Ensure it’s the domain you want

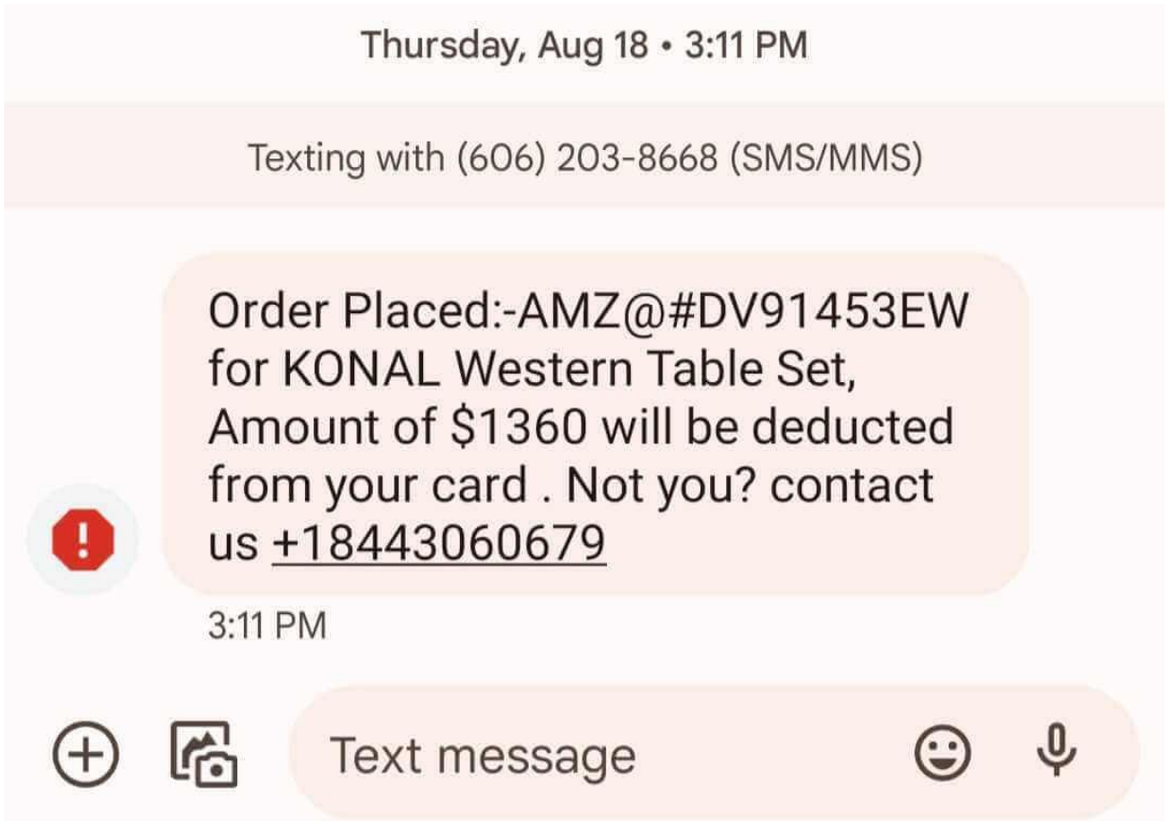
Real Life Scenario

- Website displays pop up
- Victim calls number on screen
- Scammer tells them someone is withdrawing money from their account
- Scammer asks victim to “Verify” name of bank
- “Transfers” to bank branch
- Attempts to “save” money by transferring money out of account



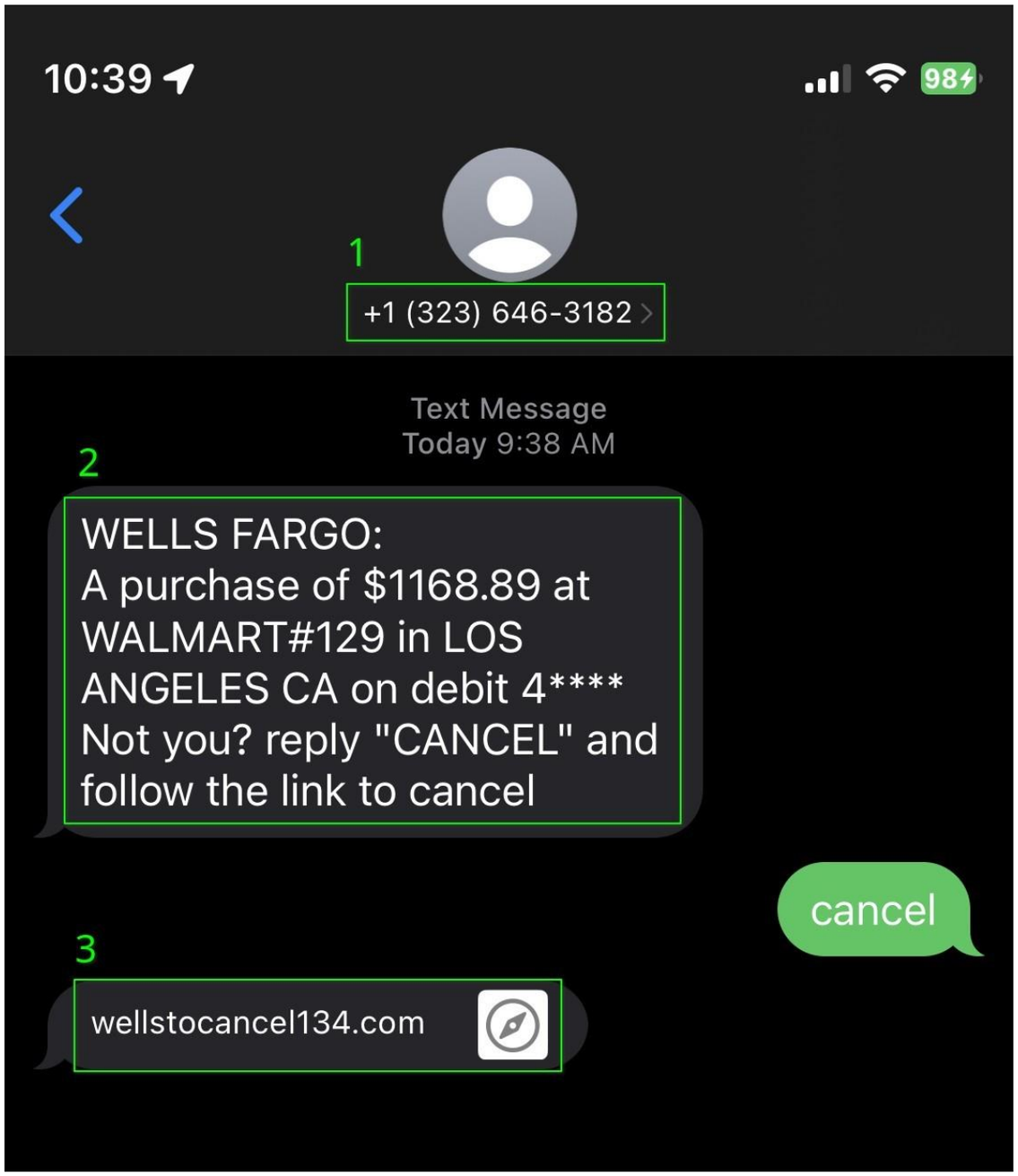
Real Life Scenario

1. Victim receives a text message about a purchase using their credit card
2. Victim calls number on screen
3. Scammer tells them someone is using their credit card
4. Scammer asks you to “Verify” name of bank
5. Scammer asks for victim credentials to “verify” identity
6. Scammer makes purchases or orders a new credit card



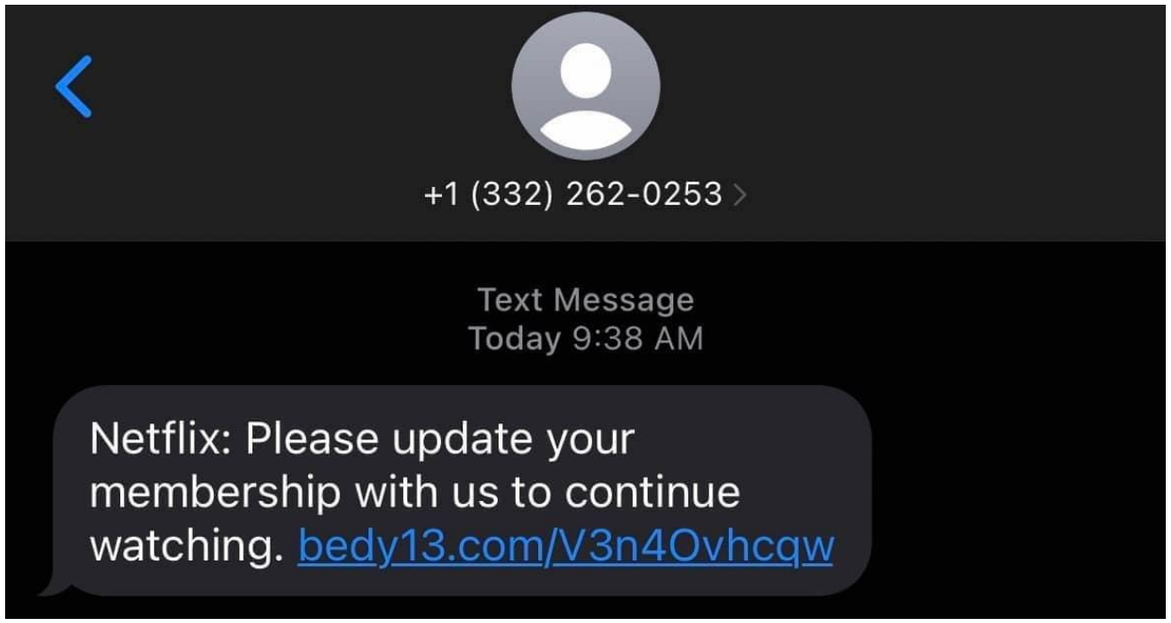
Real Life Scenario

- Victim receives a text message about a purchase using their debit card
- Victim follows visual cues to cancel the charge
- Scammer sends link
- Victim uses link and is prompted to login using bank credentials



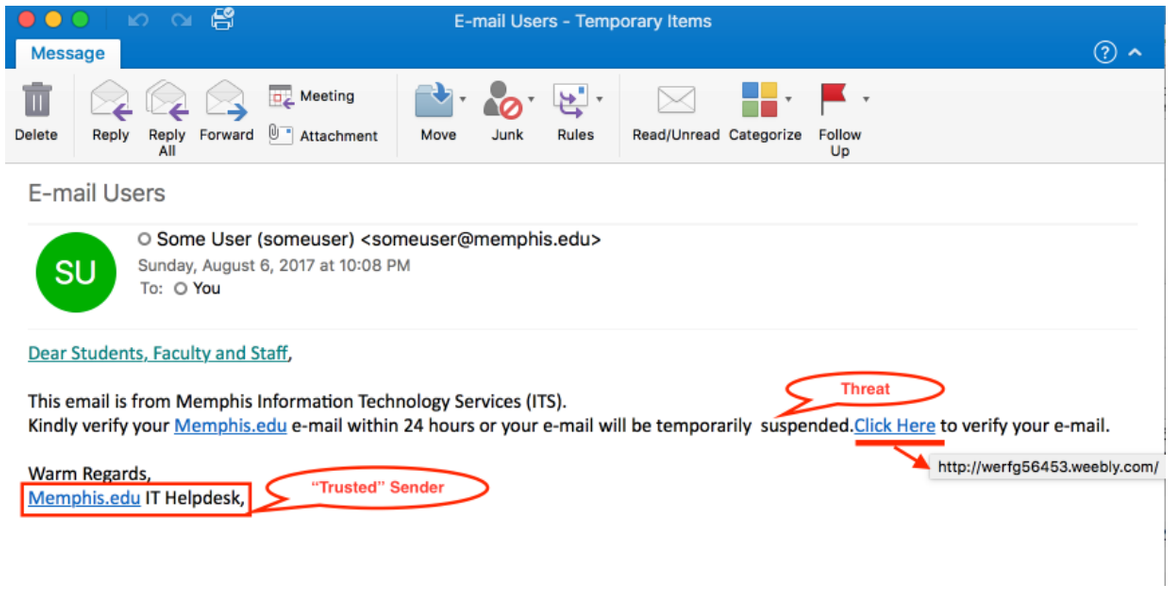
Real Life Scenario

- Victim receives a text message about keeping an account current
- Victim follows provided link
- Victim uses link and is prompted to login using account credentials



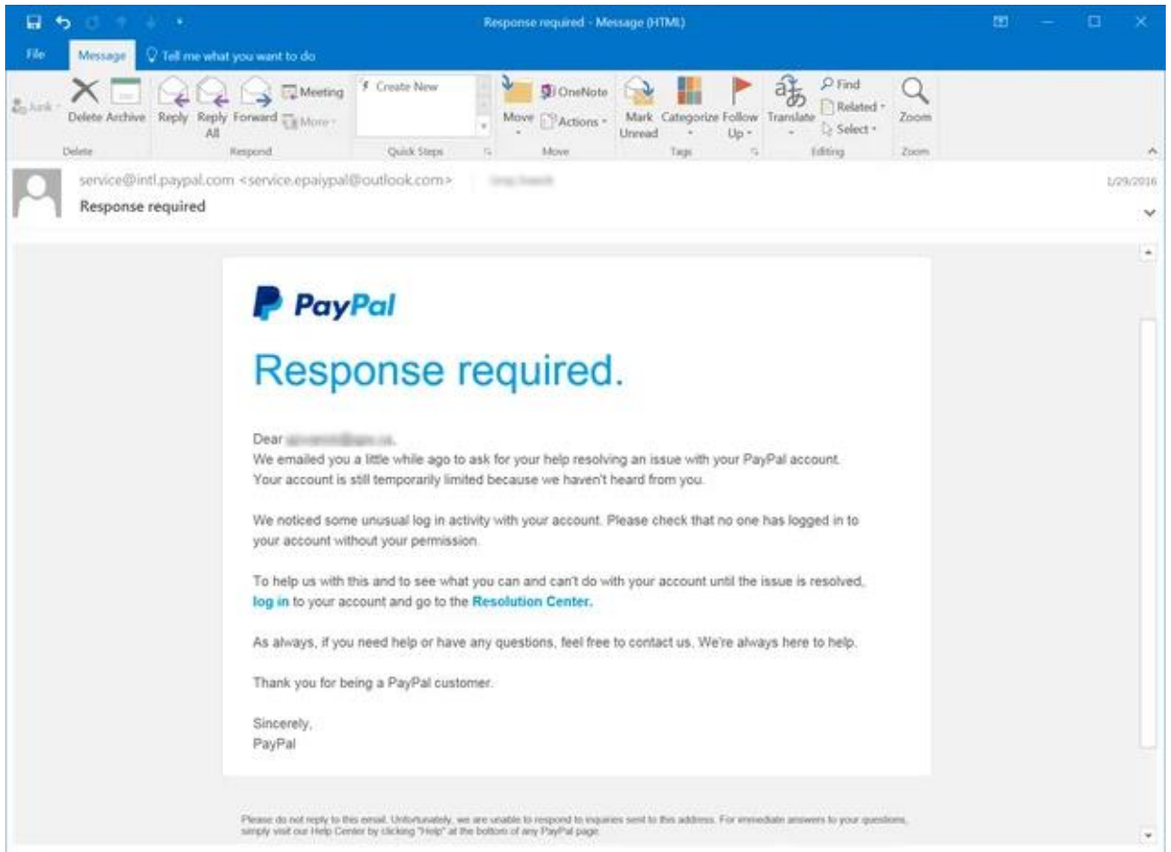
Real Life Scenario

- Victim receives an email about keeping an account current
- Victim follows provided link
- Victim uses link and is prompted to login using account credentials



Real Life Scenario

- Victim receives an email about keeping an account current
- Victim follows provided link
- Victim uses link and is prompted to login using account credentials



Real Life Scenario

- Victim receives an email asking about availabililty
- Victim responds
- Scammer asks victim to make a gift card purchase and send details

From: Alex Miltiades <desskoffice22@gmail.com>
Date: Thursday, June 13, 2024 at 10:02 AM
To: Dr. Andy Green <andy@andy-green.org>
Subject: <no subject>

Andy

Are you available at the moment?

Regards.

NEVER DO THIS

What do these all have in common?

1. APPEAR to come from a trusted source
2. Creating a sense of urgency
3. Threats of negative outcome if action not taken
4. Requests for help

SO, WHAT DO WE DO ABOUT THIS?

Know who you are talking to

Never give information out to someone who calls, texts or emails without verifying the channel of communication

Use Unique Passwords

Do not reuse passwords.

Use a password manager. Yes, a notebook and pen/pencil is ok!

Use Unique Passwords

At least use different passwords for your banking and email accounts.

Please?

Enable Multifactor Authentication (MFA)

MFA prevents people from logging into accounts even if they have your credentials. A code is sent to your email or phone as an extra security measure.

It’s typically under account> Security settings. You may need to look for it.

The two biggest combinations of factors you can employ to protect yourself in everyday life are using unique passwords and enabling MFA where available.

Conclusion

- Stay vigilant
- Listen to your gut
- Slow down
- Talk to someone if you're unsure

Email: agreen@holytransfiguration.info

Slides - https:/andygreen.phd/presentations